

ABSTRACT OF THE DISCLOSURE

In the chaining key broadcasting reception system, a chaining key reception unit receives a chaining key, an identifier of the key in question and a target key identifier indicative of a chaining key to be decoded by the key in question[[],]; a chaining key management unit takes out an already stored chaining key by using the target key identifier received by the chaining key reception unit[[],]; and a chaining key decoding unit decodes the chaining key received by the chaining key reception unit by using the chaining key sent from the chaining key management unit to generate a new chaining key.